Microsoft Windows NT 5.0
System Policies

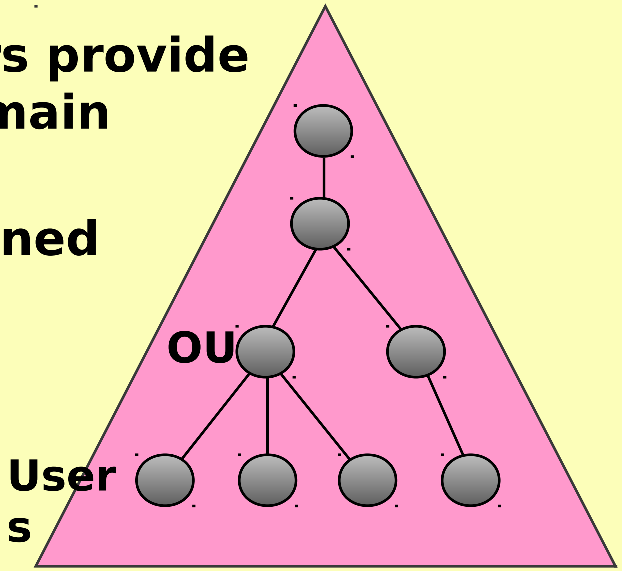
Lara M. Sosnosky
June 19, 1998

Status of NT 5.0

- **Beta Status**
  - **Beta 1 (Build 1671) - October 1997**
  - **Interim Developers Release (Build 1773) - March 1998**
  - **Interim Developers Release (Build 1814) - June 1998**
  - **Beta 2 due out end of summer**
- **Final release maybe mid-1999**
- **This presentation is based on Interim Developers Releases and Microsoft presentations (PDC, TechEd), covers:**
  - **System policies**
  - **Microsoft Management Console (MMC)**
  - **Active Directory Services Interface (ADSI)**
  - **IPSEC**

Active Directory Review

- Service that provides a comprehensive directory of objects
  - Includes all object information of interest outside the current system (users, printers, certificates)
- Active Directory (AD) is a tightly integrated component of the NT 5.0 operating system
  - Every Domain Controller (DC) hosts a copy of the Directory
- Organizational Unit (OU) containers provide finer granularity than previous domain architecture
  - Just a node or container, no defined semantics as with X.500 OUs
  - OUs can contain groups of users, machines, printers and have policies applied to them



NT Policies

- Policies vs. profiles
  - Profiles contain user environment and preference settings
    - Desktop colors, screen saver, My Documents, etc.
    - May or may not roam from machine to machine
    - Usually modifiable by user
  - Policies define what a user can do
    - Created by Administrator
    - Control what programs users can run and access
    - Not modifiable by user

Types of NT 5.0 Policies

- Types of policies in NT 5.0
  - Application policy controls what programs a user has and can run
  - Security policy controls object access, authentication
  - System policy controls shell behavior, user environment
- Locations of policies
  - Group policy is a collection of application, security, and system policies that apply to members of a site, domain, or OU
  - Local policy is a collection of policies that are cached on a workstation for use during detached operation

Application Policies

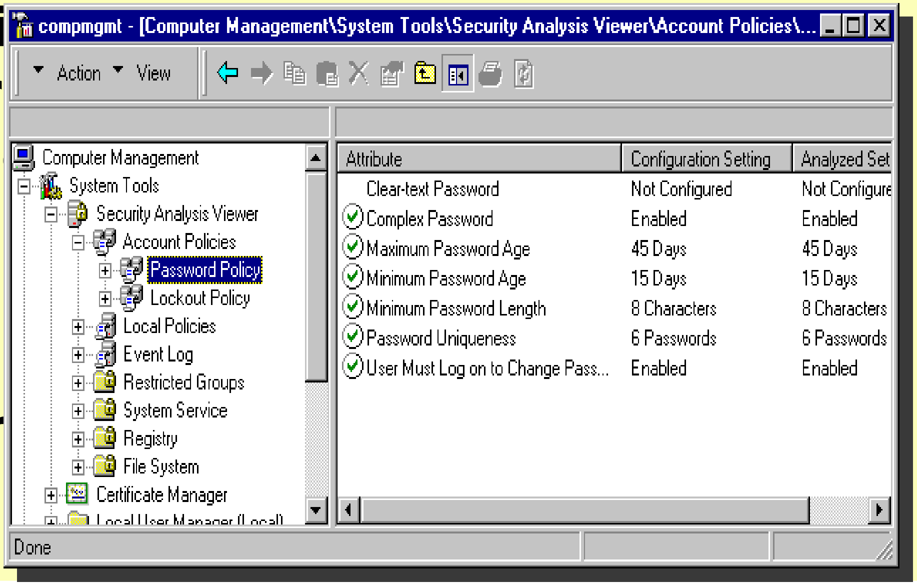
- Enhanced for NT 5.0
  - Works with Microsoft Software Installer (MSI)
- Administrator can assign applications to users
  - Assigned applications appear on the user's desktop or in their Start menu
  - When user runs program for first time, MSI kicks in and installs necessary program files on the workstation
  - User cannot delete the application icon
- Administrator can publish applications
  - Users can see and install the applications through the Add/Remove applet in Control Panel
  - Supports network installation option, so no files have to go on user's workstation
  - User can uninstall the application

Security Policies (1 of 2)

- Covers all areas of system security
  - Account policies (passwords, account lockout, Kerberos policy)
  - Auditing
  - User Rights
  - Restricted group membership (Administrators, Power Users)
  - Registry and file system security
  - Services (startup modes)

Security Policies (2 of 2)

- **Centralized management in NT 5.0**
- **Security configuration tool kit**
  - ***Security Configuration Editor (SCE)*** **- Define template with desired settings for all security areas**
  - ***Security Configuration Manager (SCM)*** **- Analyze current system setti template settings fr SCE, export and sav configuration**
  - ***Group Policy Editor (GPE)*** **- Propagate configuration as par of the group policy**



Attribute	Configuration Setting	Analyzed Set
Clear-text Password	Not Configured	Not Configure
✓ Complex Password	Enabled	Enabled
✓ Maximum Password Age	45 Days	45 Days
✓ Minimum Password Age	15 Days	15 Days
✓ Minimum Password Length	8 Characters	8 Characters
✓ Password Uniqueness	6 Passwords	6 Passwords
✓ User Must Log on to Change Pass...	Enabled	Enabled

System Policies

- Covers policies that affect all users and computers in the domain
- Same policies that we have today in NT 4.0, with additions for NT 5.0
  - User environment (Start menu, Network Neighborhood)
  - Shell access
  - Registry access
  - Logon banners
  - Logon/logoff scripts
  - IPSEC
  - Trusted certificate lists
  - Encrypting Data Recovery Policy (EDRP)
- Managed with NT 4.0 System Policy Editor or GPE

Group Policies

- Local vs. group policies
  - Local policies are defined on local machine and include Admin roles, auditing, local user rights
  - Group policies are defined in GPE and are stored in Group Policy Objects (GPOs) “Blobs of Policy”
    - Filtered by security group membership
- Group policies can include:
  - Application and file deployment policies
  - Logon/Logoff scripts, Startup/Shutdown scripts
  - Network policies (IPSEC)
  - Local policies (account lockout, password policies)
  - Computer policies (auditing, user rights)
- Can have multiple GPOs

Group Policy and AD

- ADS is the delivery vehicle for group policies
  - Policies can be applied to Site(s), Domain(s), Organization Unit(s) - (SDOU)
    - By default, policy affects all computers and users in the specified container
    - More granular than NT 4.0 policies, which were applied to entire domains
  - Stored in GPO per domain (does not transcend beyond the domain)
- Management of policies may be delegated
  - Per SDOU and/or GPO
  - Per machine

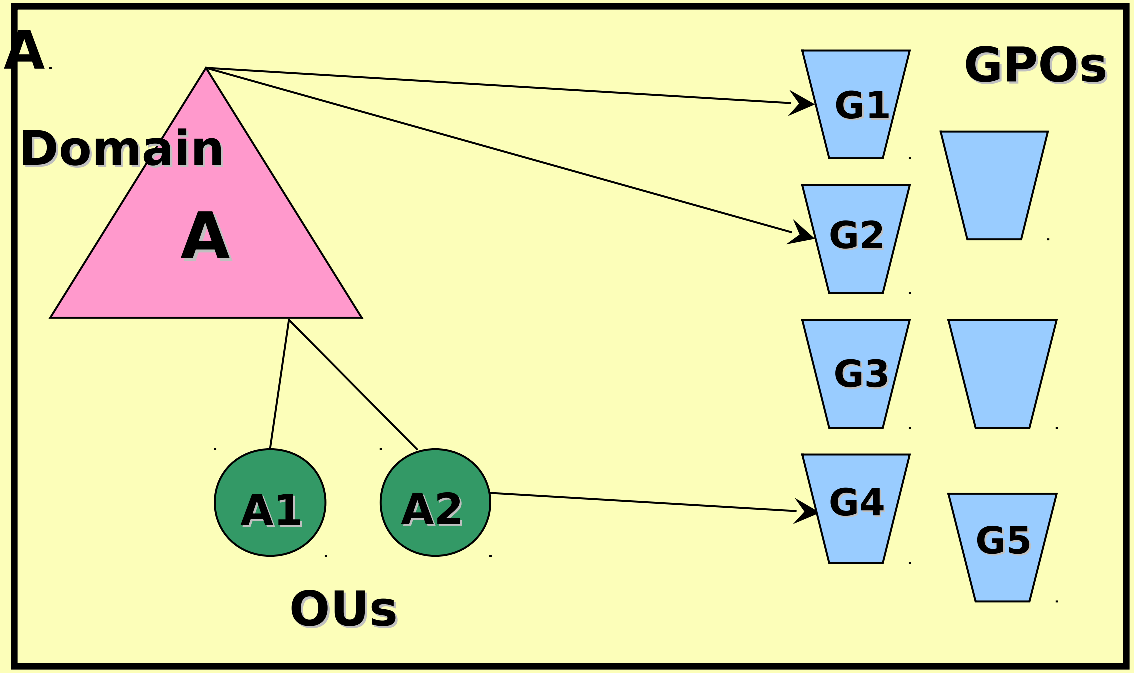
Applying Policies (1 of 2)

- Defined order:
  - Local machine policy (if no DC available, need local policy with cached credentials)
  - Site policy (area of network that is well-connected, no direct correspondence to domain necessary)
  - Domain policy
  - OU policy
- Security policy (group membership) acts as filter for group policy
  - At logon, AD is searched for all applicable GPOs
  - If user is denied access to that GPO, it will not apply

Applying Policies (2 of 2)

- **Multiple SDOUs may use a single GPO**
- **Likewise, multiple GPOs may be associated with a single SDOU**

- **User in Domain A has G1, G2**
- **A2 has G1, G2, and G4**
- **Group policy is not inherited across domains**
- **Group policy is cumulative**

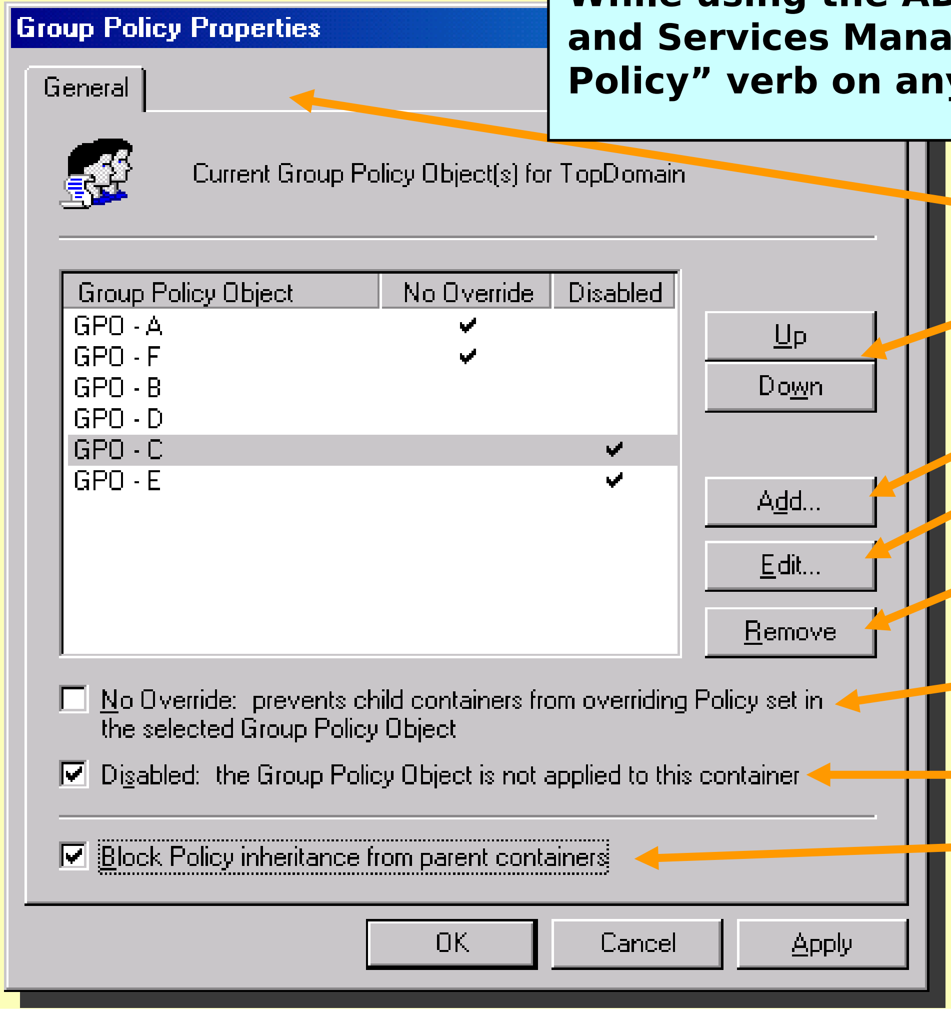


Policy Inheritance Rules

- By default, policy is inherited - where there are conflicts the most recent policy applied has the last say
- Exceptions to inheritance rules
  - Mandated (enforced) policy
    - Prevents child OUs from blocking or overriding the policy
  - Block policy
    - Blocks policy inheritance at any domain or OU
- Policy filtered by security group membership
  - Computers and users may be in same security group
- Can enable/disable policies as needed and set priorities
  - Allows great flexibility

Managing Group Policy

While using the AD Manager and the AD Site and Services Manager the "Manage Group Policy" verb on any SDOU shows this dialog



Group Policy Properties

General

Current Group Policy Object(s) for TopDomain

Group Policy Object	No Override	Disabled
GPO - A	✓	
GPO - F	✓	
GPO - B		
GPO - D		
GPO - C		✓
GPO - E		✓

☐ No Override: prevents child containers from overriding Policy set in the selected Group Policy Object

☑ Disabled: the Group Policy Object is not applied to this container

☑ Block Policy inheritance from parent containers

Security - set ACLs

Change priority

Add - GPOs to list

Edit - launches the GPE

Remove - GPOs from list or delete

No Override of policies for a GPO

Disable - GPO

Block from Parents - does not apply on sites

Start Planning

- Windows NT 4.0 Service Pack 4 (release this summer)
  - Security configuration editor
    - With built-in analysis tool
  - No group policy support
    - Use secedit.exe with SMS
- Windows NT 5.0
  - Complete tool set (SCE, SCM, GPE, MSI)
- Start planning for Active Directory
  - Analyze domain structure (sites, OUs)
  - DNS (no more WINS needed with NT 5.0!)
  - Group memberships and policies

Resources

- Windows NT 5.0 information
  - http://www.microsoft.com/ntserver/guide/nt5.asp
- Microsoft NT server white papers
  - http://www.microsoft.com/ntserver/guide/pdcwp.asp
- Management information
  - http://www.microsoft.com/management
  - http://www.microsoft.com/zaw
  - http://www.microsoft.com/management/mmc/overview.htm
- Active Directory information
  - http://www.microsoft.com/ntserver/guide/activedirectory. asp
- Microsoft conferences
  - Professional Developers Conference (PDC) - October 12-15